UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

DARRYL BOWSKY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ELEKTA INC.; and NORTHWESTERN MEMORIAL HEALTHCARE

Defendant(s).

Case No.

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff DARRYL BOWSKY ("Plaintiff" or "BOWSKY") brings this Class Action Complaint against Defendants ELEKTA, INC. ("ELEKTA") and NORTHWESTERN MEMORIAL HEALTH CARE ("NMHC") in his individual capacity and on behalf of all other similarly situated individuals. He alleges with personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from Defendants' individual and collective failures to secure and protect Plaintiff's and Class Members' Sensitive Information from unauthorized disclosure to criminal third parties. There are three types of Sensitive Information at issue in the case: (1) personal identifying information ("PII"), including names, Social Security Numbers, dates of births, and addresses; (2) protected health information ("PHI"), including cancer treatment records, medical record numbers, medical histories, dates of service, treatment plans, and health insurance information; and (3) and protected genetic information ("PGI") including

genetic testing and DNA analysis that was provided to Defendants during cancer treatment care and as participants in clinical trials related to cancer treatment. The specifics of the compromised data and extent of the forensic investigation is in the exclusive control of defendants and their agents and unavailable to Plaintiff absent discovery.

2. PII, PHI and PGI are collectively referred to herein as "Sensitive Information."

3. Cancer is a genetic disease -that is, cancer is caused by certain changes to genes that control the way our cells function, especially how they grow and divide. Certain gene changes, or mutations, can cause cells to evade normal growth controls and become cancer. For example, some cancer causing genes change or increase the production of a protein that makes cells grow.[1] Genetic tests for hereditary cancer can help determine whether certain patients are more susceptible to developing certain types of cancer and whether patients will respond to certain types of medications.

4. As part of the ongoing development of science and medicine, and during the treatment course, "oncology clinics around the world generate enormous amounts of data."[2] In an effort to support and streamline the data from multiple sources to improve patient care and research, Elekta maintains a first-generation cloud-based data storage system that serves cancer healthcare providers. The cloud-based system is integrated with Elekta software to help medical professionals with patient management by providing a "complete picture" of the patient and their care pathways.

5. Elekta promotes its products as a "single source of clinical truth" [3] and offers a "suite of cloud based clinical and business intelligence applications" that (1) collect, aggregate, an

[1] https://www.cancer.gov/about-cancer/causes-prevention/genetics
[2] https://www.elekta.com/software-solutions/knowledge-management/registries/data-alliances
[3] https://www.elekta.com/software-solutions/#care-management

analyze information from multiple data systems; (2) use real time dashboards for effective analysis to improve practice; and (3) ensure compliance and support research with standardized data collection and reporting. [4]

6. Between April 2, 2021 and April 20, 2021, Elekta experienced a ransomware attack and subsequent data breach that allowed hackers to gain unauthorized access to Elekta's cloud-based radiology software ("Data Breach") that allowed access and extractions of the personal and medical information of oncology patients throughout the United States.

7. Due to Elekta's inadequate data security, which failed to comply with federal and state law and failed to meet industry data privacy standards, an unauthorized third party used compromised credentials to gain access to Elekta's digital environment. Thereafter, the unauthorized third-party gained access to, and then exfiltrated, the files and records of various businesses customers of Elekta, including Northwestern Memorial HealthCare, Renown Health, St. Charles Health System, Carle Health, Cancer Centers of Southwest Oklahoma, LLC, Lifespan, Southcoast Health, and Yale New Haven Health.

8. In response, Elekta engaged in a forensic investigation on or about April 28, 2021 and thereafter announced that "Elekta must conclude that all data within Elekta's first-generation cloud system was compromised." [5] Upon information and belief, the files and records that were accessed and exfiltrated and compromised included the Sensitive Information of Plaintiff and the Class Members.

9. Healthcare providers and their vendors, including Defendants, that collect and store Sensitive Information of their patients have statutory, regulatory, and common law duties to

[4] https://www.elekta.com/software-solutions/#knowledge-management
[5]https://www.saintpetershcs.com/News/2021/Saint-Peter%E2%80%99s-University-Hospital-Notified-of-Data

safeguard that information and ensure that it remains private and protected against foreseeable criminal activity.

10. Defendants breached their statutory, regulatory, common law and contractual duties as discussed herein.

11. Defendant Northwestern also expressly and impliedly promised Plaintiff and its other patients that it would maintain the privacy and confidentiality of Plaintiffs and Class Members Sensitive Information.

12. Defendant's patients, including Plaintiff, entered into implied contracts with Defendant NMHC as part of their medical services and involvement in clinical trials whereby Plaintiff and Class Members reasonably expected that the Sensitive Information they entrusted to their healthcare provider would remain confidential and would not be shared or disclosed to criminal third parties. The implied promises included an understanding that Defendant NHMC would take steps to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information. Defendant, individually and by and through its agent Elekta, breached these contractual duties by failing to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information.

13. As a result of Defendants collective failures to implement and follow reasonable security procedures, the Sensitive Information is now in the possession of criminal networks placing Plaintiff and the Class Members at risk for identity theft. Plaintiff and Class Members have suffered numerous actual, concrete, and imminent injuries as a direct result of the Data Breach, including, but not limited to: (a) theft of their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with the time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the

consequences of the Data Breach; (d) the emotional distress, stress, nuisance, and annoyance of the responding to and resulting from the Data Breach; (e) the actual and/or imminent injury arising from the actual and/or potential fraud and identity theft posed by their Sensitive Information being placed in the hands of the ill-intentioned hackers and/or criminals; (f) damages to and diminution of value of their Sensitive Information entrusted to Defendant; (g) the actual damages in the difference between the services that should have been delivered and the services that were actually delivered; (i) the continued risk to their Sensitive Information and personal identity, which requires further protection; (j) and statutory damages provided under 410 ILCS 513 ("Genetic Privacy Act").

JURISDICTION & VENUE

14. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant Elekta, there are more than 100 putative Class Members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

15. This Court has specific jurisdiction over Defendant Elekta because Elekta intentionally availed itself of this jurisdiction by marketing and selling products and services to many businesses nationwide and in the State of Illinois, including to co-Defendant NHMC. This court has jurisdiction over NMHCC because NMHC A/K/A Northwestern Medicine is an Illinois Non-Profit corporation at home in Illinois.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

17. Plaintiff BOWSKY is a natural person and a citizen of Illinois and a resident of Cook County, Illinois. Plaintiff BOWSKY is careful about sharing his Sensitive Information, and he has never knowingly transmitted his Sensitive Information over the internet or any other unsecured source.

18. In July 2021, Plaintiff received a Notice letter dated June 25th, 2021 informing him that his PII/PHI had been compromised and stolen in a cyberattack. The Notice letter confirmed that data involved in the cyberattack contained Plaintiff's PII and PHI that has been provided to NMHC during the course of his medical care. This notice was particularly concerning to Plaintiff who was a cancer patient who underwent biopsies, and resection procedures that may have involved genetic testing. Plaintiff was also a volunteer for a clinical trial involving DNA testing, acquisition, storage and analysis related to cancer treatment.

19. As a result of the Notice, Plaintiff has experienced annoyance, emotional distress, and he has lost time and opportunity cots by reviewing his financial accounts and researching the impact of the data breach. He will be spending additional time reviewing his medical information for medical identity theft and continuing to monitor his financial accounts. Furthermore, Plaintiff is concerned and suffering emotional distress related to whether his DNA information was accessed and exfiltrated during the Breach.

20. Defendant ELEKTA is a Swedish radiation therapy, radiosurgery and related equipment and data services provider with its principal place of business in Dunwoody, GA and conducts business throughout the United States including Illinois. Service of Process is proper on Illinois Corporation Service C at 801 Adlai Stevenson Dr., Springfield, Illinois 62703.

21. Defendant NMHC A/K/A Northwestern Medicine is an Illinois Non-Profit

corporation and integrated health system offering patients access to hundreds of locations including eleven hospitals throughout the Chicagoland area.[6] It also offers clinical studies in a broad range of studies including cancer care. [7] Service of process is proper on Danae K. Prousis at 211 E Ontario St., Suite 1800, Chicago, IL 60611.

GENERAL FACTUAL ALLEGATIONS

22. As a condition of engaging in health services or clinical trials, Defendant NMHC requires that these persons entrust them with Sensitive Information. The PII and PHI is subsequently shared with its vendor and agent Elekta. Upon information and belief, PGI that is gathered and utilized during the care and treatment of cancer patients is also shared and utilized on the Elekta platform to help coordinate patient care.

23. Elekta describes itself as "a global leader in radiotherapy solutions to fight cancer and neurological diseases." "We have a broad offering of advanced solutions for delivering the most efficient radiotherapy treatments."[8]

24. Elekta provides "cloud based" solutions that are hosted on Elekta Axis, a fully managed services cloud environment built specifically for Elekta software to improve scalability and reliability.

25. The integrated software component helps provide "access to more timely and complete patient information." It provides "better tools for sharing, analyzing, and applying information", and provides for information guided care for cancer patients. [9] And it provides the

[6]https://www.nm.org/about-us/northwestern-medicine-newsroom/media-relations/about-our-health-system (last visited September 28, 2021)

[7] https://www.nm.org/conditions-and-care-areas/clinical-trials-and-research (last visited September 28, 2021)

[8]

[9] https://www.elekta.com/software-solutions/# (last visited October 5th, 2011)

ability to "track and manage oncology treatments" including comprehensive and integrated oncology information system where the database "aggregates all of your patient data, clinical regimes, and pharmacy information". [10]

26. Without patient data to analyze and organize for medical practitioners, the software is of no value; it is the complete and comprehensive data provided exclusively by Plaintiff and those he seeks to represent that creates value for the Elekta system.

27. Genetic testing and DNA data is part of a patient profile and is routinely used in oncology practices to select treatment plans and prescriptions for cancer patients. Specific genetic changes can be used to predict which patients are likely to have a better or worse outcome and are part of a patient's medical history.

28. In order to acquire this data, gene expression panels are performed on samples of the cancer. These panels are available for a number of types of cancer including breast, colon, and prostate cancers and can help predict which patients are more likely to recur. [11]

29. The genetic information can also be utilized when prescribing certain medications. Some drugs will not work if the patient has certain gene mutations. The most well-known example is HER2 positive breast cancer, where patients do not respond as well to certain chemotherapy drugs. But newer drugs such as Herceptin have been specifically designed to attack HER2 positive cancers. Breast cancers, therefore, are routinely genetically tested to identify which patients will benefit from these drugs. [12]

30. Biomarker testing is also a common practice that is utilized to help a physician

[10] https://www.elekta.com/software-solutions/care-management/mosaiq-medical-oncology
[11] https://www.cancer.org/cancer/cancer-causes/genetics/genes-and-cancer/genes-in-cancer-diagnosis-and-treatment.html
[12] Id.

select an appropriate treatment course. During biomarker testing, the health care provider will look for genes, proteins, and other substances or tumor marks that provide information about the cancer. Some cancer treatments including targeted therapies and immunotherapies, may only work with certain biomarkers. Biomarker testing is routine for patients with certain types of cancer including non-small cell lung cancer, breast cancer, and colorectal cancer. [13]

31. Biomarker testing may also be called tumor testing, tumor genetic testing, genomic testing, molecular testing, somatic testing, and tumor subtyping.

32. There are also many clinical trials that acquire genetic information as part of the trial. Plaintiff was recruited and participated in one such study where his genetic information and DNA was provided to NHMC.

33. Recognizing that the treatment of cancer is "complex and data driven," Elekta has seized on the big data and artificial intelligence healthcare market to increase its revenues. The oncology software captures and leverages patient data to allow healthcare providers access to complete and relevant data aimed at automating healthcare processes and driving business decisions. The software is marketed to contain the capability to enable "precision planning" and "better predict likely outcome based on your intended plan". [14]

34. Elekta captures and stores the PII and PHI and likely the PGI of its radiotherapy clients, like NMHC, asserting that it attempts to analyze this data and improve clinical outcomes, productivity and ultimately increased financial performance of the healthcare provider. It is believed that these services, and other aspects of oncology clinical care and research, were part of the purpose for the data sharing between the Defendants.

---

[13] https://www.cancer.gov/about-cancer/treatment/types/biomarker-testing-cancer-treatment (last visited October 6th, 2021)

[14] https://www.elekta.com/software-solutions/#treatment-management

35. Moreover, while PGI and DNA data has not been confirmed or specifically disclosed by Defendants as part of the breach, the breach involves a broad and extensive breach of Elekta's cloud-based system that was specifically designed to contain comprehensive and complete medical information involving cancer patients, including Plaintiff. And Plaintiff had provided his DNA information to NMHC. As such, upon information and belief, it is plausible that PGI, including but not limited to genetic testing information such as gene expression panels and DNA data was being utilized for patient care planning through the Elekta software that was integrated with the Elekta cloud-based system that was compromised in the Data Breach.

PRIVACY WAS AN INTEGRAL PART AND A REASONABLE EXPECTATION OF THE SERVICES PROVIDED

36. Confidentiality is a cardinal rule of the provider-patient relationship.

37. Plaintiff and Class Members are aware of a medical provider's duty of confidentiality, and as a result, have an objective reasonable expectation that NMHC will not share or disclose, whether intentionally or unintentionally, Sensitive Information in the absence of authorization for any purpose that is not directly related to or beneficial to patient care.

38. Likewise, pursuant to HIPAA and industry standards, medical providers understand that the services they provide to patients includes confidentiality.

39. Elekta specifically markets and holds itself out as being committed to Cybersecurity stating: "In today's interconnected digital healthcare ecosystem, the highest cybersecurity standards are critical for patient safety and data protection." [15] Elekta further markets itself as being "committed to advancing cybersecurity in medical devices and maintaining the protection of

[15] https://www.elekta.com/software-solutions/product-security (last visited October 5th, 2021)

patient, personal and business data." [16]

40. As detailed more fully below, Defendants failed to safely and securely store the Sensitive Information entrusted to them and failed to prevent it from being compromised during the Data Breach.

The Breach

41. In late April 2021, Elekta was the subject of a ransomware attack that targeted its cloud-based systems that hosted and maintained oncology and radiology data. It was determined that the PII and PHI provided to Elekta by certain of its oncology and radiology healthcare clients was compromised, including Plaintiff's and Class Members' Sensitive Information. Upon information and belief, Plaintiff's and Class Members PGI was also exposed and compromised.

42. Shortly thereafter, Elekta began emailing its clients, including NMHC, that it was taking action to immediately cut off the cyberattackers by temporarily taking its systems offline and cancelling or rescheduling radiation treatment appointments for cancer patients.

43. And in late May 2021, Elekta began notifying its healthcare clients that their clinical information containing the PII and PHI of patients may have been compromised in the ransomware Data Breach.

44. Soon after the breach notification, an Elekta representative explained:

> Elekta was subjected to a series of cyberattacks which affected a subset of U.S.-based customers on our first-generation cloud system. On April 20, to contain and mitigate the attacks, Elekta proactively took down its first-generation cloud system in the United States. An investigation is being conducted, and any affected customer(s) will be contacted and fully briefed through the appropriate channels and in accordance with any legal requirements.[17]

[16] https://www.elekta.com/software-solutions/product-security (last visited October 5th, 2021)
[17]https://compliancy-group.com/healthcare-vendor-ransomware-attack-170-health-systems-hit/ (last visited July 14, 2021)

45. Elekta's healthcare clients then began notifying their patients, including Plaintiff and Class Members. For example, in June 2021, Northwestern Memorial HealthCare notified approximately 201,197 patients that "an unauthorized individual gained access to [Elekta's] systems between April 2, 2021 and April 20, 2021 and, during that time, acquired a copy of the database that stores some oncology patient information."[18] Additionally, on or about June 25, 2021, Renown Health notified approximately 65,181 patients that "[w]e are writing to inform you of a recent data security incident that involved our business associate, Elekta, Inc. ('Elekta')."[19]

46. Additional data breach notifications went out to other Elekta clients such as Cancer Centers of Southwest Oklahoma, Carle Health, Lifespan, Charles Health System, Yale New Haven Health, Emory Healthcare and Southcoast Health. In total, approximately 42 healthcare systems are believed to have been affected by the Data Breach that happened on Elekta's watch.

47. The various data breach notices have indicated the stolen PII and PHI included full names, Social Security numbers, addresses, dates of birth, height, weight, medical diagnoses, medical treatment details, appointment confirmations, and other personal and protected information. Specifically, Plaintiff's notice indicated the data involved in the Data Breach "may have included patient names, dates of birth, Social Security numbers, health insurance information, medical record numbers, and clinical information related to cancer treatment, such as medical histories, physician names, dates of service, treatment plans, diagnoses, and/or prescription information." [20]

[18] https://www.nm.org/patients-and-visitors/notice-of-privacy-incident (last visited July 14, 2021)
[19] file:///C:/Users/nprosser/Downloads/Elekta_Media-Notice%20(1).pdf (last visited July 14, 2021)
[20] Ex. A.

DEFENDANTS' CONDUCT VIOLATED HIPAA, FEDERAL TRADE COMMISSION & INDUSTRY STANDARDS ON DATA SECURITY PRACTICES

48. By obtaining, collecting, and using Plaintiff's and Class Members' Sensitive Information in the procurement and provision of services to Plaintiff and Class Members, and ultimately deriving benefit therefrom, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Sensitive Information.

49. Defendants owed numerous statutory, regulatory, and common law duties to Plaintiff and Class Members to keep their Sensitive Information confidential, safe, secure, and protected from unauthorized disclosure or access, including duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

HIPAA Standards & Violations

50. Upon information and belief, Defendants each failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of its customers' personal information in compliance with industry recognized cybersecurity framework and HIPAA.

51. The Data Breach resulted from a combination of insufficiencies that indicate the Defendant failed to comply with safeguards mandated by Federal and State Law and industry standards. The security failures included but are not limited to:

A. Failing to maintain an adequate security system to prevent data loss;

B. Failing to implement policies and procedures that limit use and disclosure of PII and PHI to its vendors to the minimum necessary;

C. Failing to mitigate the risks of data breach and loss of data;

D. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. 164. 306(a)(1);

E. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access to only those persons or software programs that have been granted access in violation of 45 C.F.R. 164.312(a)(1);

F. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violations of 45 C.F.R 164.308(a)(1);

G. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

H. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

I. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

J. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

K. Releasing, transferring, allowing access to, and divulging protected Sensitive Information to unauthorized criminal third parties.

FTC Guidelines & Violations

52. The Defendants also failed to comply with Federal Trade Commission ("FTC") Guidelines.

53. The Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

54. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed for authorized purposes; encrypt information stored on computer networks, understand their networks vulnerabilities; and implement policies to correct any security problems.[21]

55. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[22]

56. The FTC further recommends that companies not maintain Sensitive Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords; use industry tested methods for security; monitor for suspicious activity on the network; and verify that third party providers, such as Elekta, have implemented reasonable security measures. [23]

57. The FTC has brought enforcement actions against businesses for failing to

[21] Federal Trade Commission, Protecting Personal Information: A Guide for Business, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 24, 2021)

[22]https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf (last visited May 21, 2021)

[23] Federal Trade Commission, Start With Security, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited September 24th, 2021)

adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

Industry Standards & Violations

59. Defendants' failures also violated industry standards for data security practices. [24]

60. HHS's Office for Civil Rights ("DHHS") highlights several basic safeguards that are easily implemented to improve cybersecurity in the healthcare industry. These steps include: (1) proper encryption of Sensitive Information; (2) educating and training healthcare employees and agents on how to protect Sensitive Information; and (3) correcting the configuration of software and network devices.

61. Upon information and belief, Defendants breached some or all of these steps allowing vulnerabilities in Elekta system that contributed to the data breach.

THE DATA BREACH WAS FORESEEABLE.

62. It is well known that Sensitive Information, including medical information, health insurance information, dates of birth with names and addresses, and genetic information is a valuable commodity and frequent target of criminal attacks.

63. Plaintiff and Class Members, as current and former patients, and current and former

[24] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/(last accessed September 24th, 2021)

employees, relied on Defendants to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosure of this information.

64. Defendants were at all times fully aware of its obligations to protect the Sensitive Information of consumers because of its business model of collecting Sensitive Information and storing such information for analysis and for pecuniary gain. Defendants were also aware of the significant repercussions that would result from its failure to do so.

65. Elekta specifically identifies the operational risk and mentions that there needs to be an "appropriate measure[] to protect the data against damage,"[25] and further notes that there is "an increasing threat of material cyber and information security attacks targeting healthcare data,"[26]

66. And Elekta sells itself as able to "[p]rotect your data" with improved data security and AI along with multi-layer threat protection, better data organization leveraging modular infrastructure and disk encryption at rest.[27] Elekta "ensures that safeguarding your clinical data is our highest priority."

67. The medical community and Defendant NMH are aware of numerous recent data breaches on medical facilities and their vendors.

68. In May 2019, the American Medical Collection Agency (AMCA) reported that an 8-month data breach had exposed more than 20 million patients' Sensitive Information. This event brought into focus the risk faced when healthcare providers work with outside vendors and allow access to their systems.

[25] *Id*. at 35.
[26] *Id.* at 98.
[27] https://www.elekta.com/software-solutions/cloud-solutions/ (last visited July 14, 2021)

69. And according to the United States Cybersecurity & Infrastructure Security Agency:

> Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations. https://www.cisa.gov/ransomware (last visited Apr. 16, 2021).

70. Since these warnings, healthcare-related breaches have continued to rapidly increase, and yet Defendants failed to exercise the reasonable care in hiring, training, and supervising their employees and agents to implement necessary data security and protective measures.

71. As such, Defendants should have not only known about the potential for the data breach but should have taken steps to increase the security. Instead, they relied on their outdated safeguards leading to the inevitable breach.

THE DATA BREACH WAS PREVENTABLE

72. Data breaches are preventable.[28] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[29] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not

[28] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).

[29] *Id.* at 17.

compromised."[30]

73. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[31]

PLAINTIFF AND CLASS MEMBERS ARE AT AN INCREASED RISK OF IDENTITY THEFT AS A DIRECT RESULT OF DEFENDANT'S ACTIONS

74. The risk of identity theft is real and concrete and not hypothetical. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

75. According to industry experts, one out of four data breach notification recipients becomes a victim of identity fraud.

76. Stolen PII and PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

77. Once PII and PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the victims.

[30] *Id.* at 28.

[31] *Id.*

78. Data breaches facilitate identity theft as hackers obtain consumers' PII and PHI, thereafter using it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII and PHI to others who do the same.

79. Indeed, the Notice Letter provided by NWHC acknowledges the real and concrete risk by providing information on "Identity Theft Protection" and stating: "We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity."

80. Moreover, compromised health information can lead to falsified information in medical records and to fraud that can persist for years as medical identity fraud "is also more difficult to detect taking twice as long as normal identity theft."[32]

81. As observed in the Trend Micro analysis of the DoppelPaymer ransomware, the ransomware is not employed until the hacker has gained access to high-value information and systems. Once the hackers have secretly searched the system to their satisfaction, they execute the ransomware, which encrypts what is believed to be the most sensitive or valuable files. As a result, Plaintiff and the Class Members have the reasonable belief that their personal and medical information is now in the hands of hackers that will or already have misused their data or sold it to other criminals who have or will do so in the future.

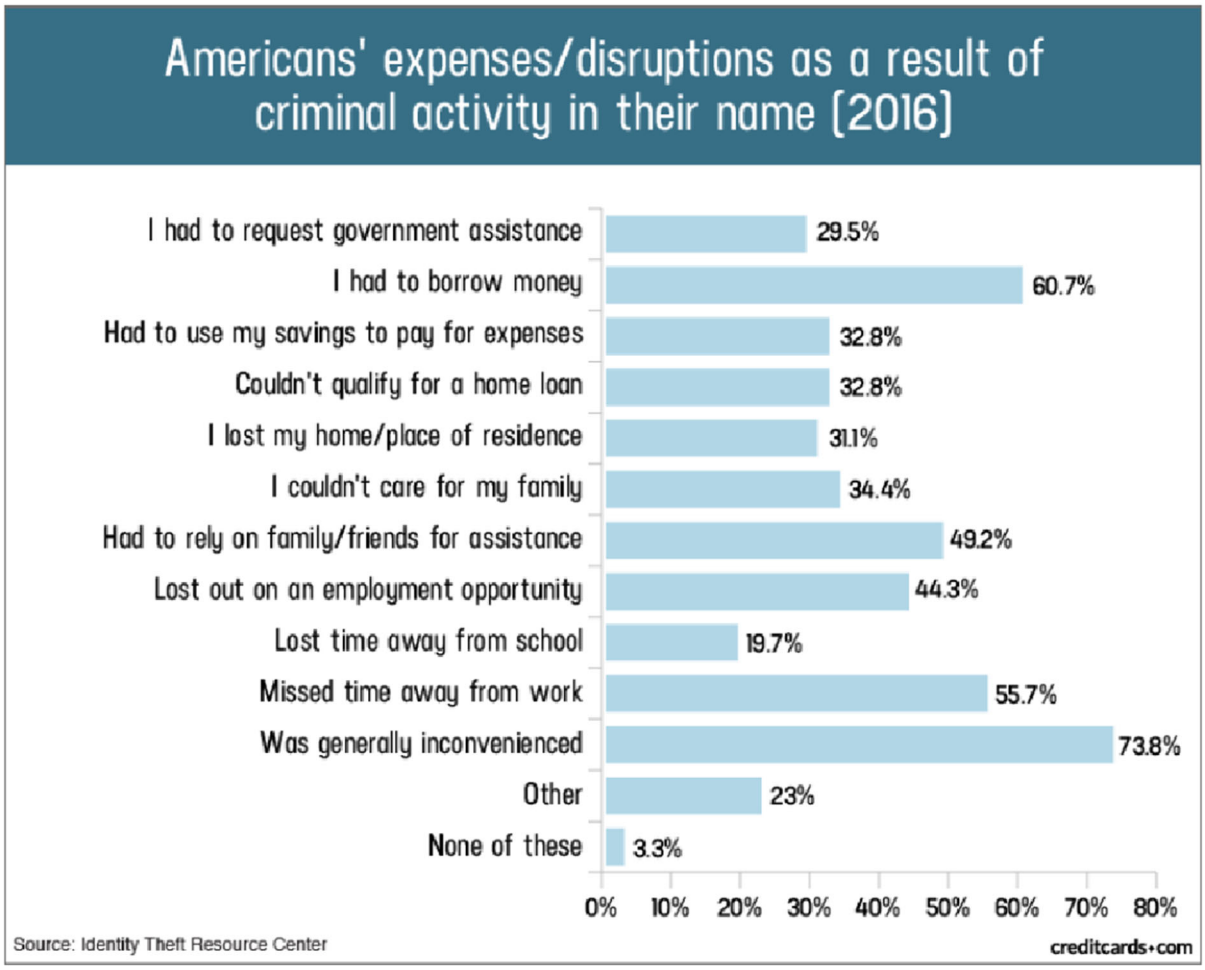
82. Identity thieves use another's personal information, including dates of birth, addresses, health insurance, and health information for a variety of crimes, including credit card fraud, phone or utilities fraud, mortgage fraud, auto loans, bank/finance fraud, disability and unemployment benefits fraud, and medical identity theft.

83. In addition, identity thieves may receive medical services in the victim's name

32

and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

84. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Apr. 19, 2021).

85. According to the Electronic Privacy Information Center:

> Identity theft is an enormous problem for consumers. The Federal Trade Commission reported 399, 225 cases of identity theft in the United States in 2016. Of that number, 29% involved the use of personal data to commit tax fraud. More than 32% reported that their data was used to commit credit card fraud, up sharply from 16% in 2015. A 2015 report from the Department of Justice found that 86% of the victims of identity theft experienced the fraudulent use of existing account information, such as credit card or bank account information. The same report estimated the cost to the U.S. economy at $15.4 billion.

The Value of the Stolen Data

86. The compromised Sensitive Information of Plaintiff and Class Members has a high value in both legitimate and black markets.

87. The FTC has recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

88. Recognizing the high value consumers place on their PII and PHI, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[33]

89. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of same. Research shows how much consumers value their data privacy,

[33] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last accessed July 14, 2021)

and the amount is considerable.

90. As a major component of its oncology and neuroscience business, Elekta maintains large volumes of its clients' Sensitive Information. As such, Elekta is well aware of the value of healthcare patient data and highly sought by cybercriminals.

91. Likewise, the Illinois general assembly recognizes that "the use of genetic testing can be valuable to the individual." [34]

92. Stolen Sensitive Information is valuable to identity thieves. The purpose of stealing large blocks of Sensitive Information, like in this Data Breach, is to use the data for illicit purposes or to sell the data for profit to other criminals who buy the data and misuse it.

93. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[35]

94. Medical data has particular value on the black marker because it often contains all of an individual's Sensitive Information, as opposed to a single marker that may be found in a more benign data breach.

95. According to a Trustware report, a healthcare data record may be valued up to $250 a record on the black market compared to $5.40 for the next highest value (a payment card).[36]

96. Healthcare related data is among the most sensitive and personally consequential when compromised. "Medical identity theft is a growing and dangerous crime that leaves its

[34] 410 ILCS 513 Sec 5(1) (Genetic Information Privacy Act)("GIPA")

[35] Javelin Strategy & Research, Identity Fraud Hits All Time High With 16.7 Million US Victims in 2017. According to New Javelin Strategy & Research Study (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (last visited May, 29th, 2021)

[36] https://www.securelink.com/blog/healthcare-data-new-prize-hackers citing https://trustwave.azureedge.net/media/16096/2019-trustwave-global-security-report.pdf?rnd=132056250120000000

victims with little to no recourse for recovery" reported Pam Dixon, executive director of World Privacy Forum.[37] A report focusing on health care breaches found that the "average total cost to resolve an identity theft related incident came to about $20,000."[38]

97. Medical information is some of the highest value data.[39] In fact, according to FBI's Cyber Division, healthcare records can be sold by criminals for 50 times the price of a stolen Social Security numbers or credit card numbers.[40] By one estimate, PHI can sell for as much as $363 according to the Infosec Institute.[41] And files containing PHI can be bought on the black market for between $1,200 and $1,300 each.[42]

98. Thus, based on the recognized statistical research, the type of data at issue, the criminal activity at issue in this case, there is a strong probability that entire batches of stolen Sensitive Information have been dumped on the black market or are yet to be dumped on the black market, placing Plaintiff and the other Class Members at an increased risk of fraud and identity

[37] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News (Feb. 7 2014), https://khn.org/news/rise-of-indentity-theft/

[38] Elinor Mills, Study: Medical Identity theft is costly for victims, CNET (Mar.3, 2010) https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

[39] Calculating the Value of a Data Breach -What are the Most Valuable Files to a Hacker" Donnellon McCarthy Enters (July 21, 2020) https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/

[40] FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusion, FBI (Apr. 8, 2014, https://publicintelligence.net/fbi-health-care-cyber-intrusions/

[41] Data Breaches: In the Health Care Sector, Center for Internet Security, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/

[42] Elizabeth Clarke, Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs, and Counterfeit Documents Secure Works (July 15, 2013), https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents

theft for many years into the future.[43]

The Breach Justifies Reasonable Mitigation Efforts

99. It is well recognized that in data breaches fraudulent activity may not show up for prolonged periods of time -potentially years after PHI and PII are divulged to third party criminals. By some accounts, forty percent of consumers discovered they were victims of medical identity theft only after they received collection letters from creditors for expenses incurred in their names.[44]

100. Despite Defendant's acknowledged failure to protect Plaintiff's and Class Members' PII and PHI, Defendants have not offered Plaintiff or Class Members adequate recourse. NMHC has offered the trivial and inadequate remedy of free credit monitoring or identity protection services for a short period of time that will not adequately protect them or compensate them for their loss.

101. In response to the risk of identity theft, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Information.

102. In an effort to follow NMHC's advice and mitigate the risk and potential losses, Plaintiff has spent time reviewing bank accounts and insurance information looking for suspicious activity, researching the Breach, and otherwise spending time on this Data Breach. Plaintiff will continue to spend time each week monitoring his accounts in the future and remains at risk for future identity theft and the unauthorized disclosure of medical information. These efforts are reasonable in light of the current and future risk of identity theft.

---

[43] https://epic.org/privacy/data-breach/equifax/ (last visited Apr. 19, 2021).

[44] The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches, Experian (Apr. 2010) https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf

103. Plaintiff's and Class Members' efforts are in line with FTC and NMHC's recommendations. The Notice specifically advised Plaintiff and the Class to review the statements sent by health insurer or healthcare provider, as well as to review account statements for unauthorized activity.

104. The FTC further recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (or an extended fraud alert that lasts for seven years if they learn someone has abused their information), reviewing their credit reports, contacting companies to dispute fraudulent charges on accounts, placing a credit freeze on their credit, and correcting their credit reports.[45]

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

105. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if their data security, or agent's data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of the breach.

106. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

107. As a result of the Breach, Plaintiff and the other Class Members must now be vigilant and review their credit reports for suspected incidents of identity theft, and educate

[45] *See* https://www.identitytheft.gov/Steps (last visited Apr. 19, 2021).

themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. The need for additional monitoring for identity theft and fraud will extend indefinitely into the future.

108. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

109. Plaintiff and the other Class Members have suffered and will suffer actual injury due to loss of time and increased risk of identity theft as a direct result of the Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiff and the other Class Members suffer ascertainable losses in the form of out-of-pocket expenses, opportunity costs, and the time and costs reasonably incurred to remedy or mitigate the effects of the Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of the Defendant;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and

L. Closely reviewing and monitoring health insurance, medical information, financial accounts and credit reports for unauthorized activity for years to come.

110. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implements reasonable security measures and safeguards to maintain the integrity and confidentiality of the Sensitive Information, including making sure that the storage of data or documents containing Sensitive Information is not accessible by unauthorized persons and that access to such data is sufficiently protected.

111. Furthermore, Plaintiff and the Class Members did not receive the value of the bargain for the medical services that were paid for, which included an agreement to keep their medical information private and confidential as part of the care and treatment.

112. And finally, as a direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

113. In addition to the remedy for economic harm, Plaintiff and the Class Members maintain an undeniable and continuing interest in ensuring that the Sensitive Information remains in the possession of Defendant is secure, remains secure, and is not subject to future theft.

CLASS ALLEGATIONS

114. **Class Definition**: Plaintiff brings this action pursuant to Fed. R. Civ. P 23, on behalf of a class of similarly situated individuals and entities ("the Class"), defined as follows:

The Nationwide Class:

> All persons residing in the United States who had their Sensitive Information compromised as a result of the Data Breach.

The Illinois Class:

> All persons residing in the State of Illinois who had their Sensitive Information compromised as a result of the Data Breach.

Excluded from the Class and Subclass are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries; (ii) the Judge presiding over this action; and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches

115. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members which can be used to provide notice.

116. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

117. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. Plaintiff is informed and believes that the proposed Class includes over 200,000 individuals who have been damages by Defendants' collective conduct as alleged herein. Class Members can easily be identified through Defendant's records, or by other means.

118. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiff and the other Class Members, which predominate over any

individual issue, including:

A. Whether Defendants adequately protected the Sensitive Information of Plaintiff and the other Class Members;

B. Whether Defendants engaged in the wrongful conduct alleged in this Complaint;

C.

Whether Defendants' conduct was unlawful;

D. Whether Defendants owed a duty to Plaintiff and the Class Members to adequately protect their Sensitive Information and to provide timely and accurate notice of the Breach;

E. Whether Defendants knew or should have known about the inadequacies of their data protection, storage, and security;

F. Whether Defendants adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the Sensitive Information of Plaintiff and the other Class Members;

G. Whether Defendants properly trained and supervised employees to protect the Sensitive Information of Plaintiff and the other Class Members;

H. Whether Defendants breached its duty to Plaintiff and the other Class Members by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect their Sensitive Information; and

I. Whether Defendants are liable for the damages suffered by Plaintiff and the other Class Members as a result of the Breach.

J. Whether Plaintiff and Class Members are entitled to recover actual and/or statutory damages;

K. Whether Plaintiff and Class Members DNA was compromised in the Data Breach.

119. **Typicality**: Plaintiff's claims are typical of the claims of the other Class Members. All claims are based on the same legal and factual issues. Plaintiff and each of the Class Members provided Sensitive Information to Defendant and the information was accessed and disseminated for sale by unauthorized hackers. Defendant's conduct was uniform with respect to all Class

Members.

120. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to the Class, and NMHC has no defense unique to Plaintiff.

121. **Superiority**: A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class Members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

122. Class certification, therefore, is appropriate under Fed. R. Civ. P 23(b)(3), because the common questions of law or fact predominate over any questions affecting individual Class Members.

FIRST CAUSE OF ACTION
NEGLIGENCE
ALL DEFENDANTS
(On behalf of Plaintiff & the Nationwide Class or alternatively, the Illinois Class)

123. Plaintiff incorporates by reference all other allegations in the complaint as if fully set forth here.

124. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class

Members Sensitive Information. Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Sensitive Information from disclosure.

125. Regardless of the purpose of sharing the sensitive information with Elekta, NMHC, individually, and/or jointly with Elekta, owed a duty to Plaintiff to protect the data against the foreseeable criminal cyber-attacks.

126. Upon gaining access to the PII and PHI of Plaintiff and members of the Class, each Defendant knew, or should have known, of the risks inherent in collecting and storing and retaining without medical purpose the Sensitive Information of Plaintiff and the other Class Members.

127. Defendants each knew or should have known of the importance of adequate security. And Each Defendant was well aware of numerous, well-publicized data breaches that exposed the Sensitive Information of individuals, including the FBI's publications of the risk of data breach on Healthcare networks.

128. Defendant Elekta actively solicited clients who entrusted Defendant with Plaintiff's and the other Class Members' Sensitive Information when obtaining and using Defendant's services. To facilitate these services, Defendant used, handled, gathered, and stored the Sensitive Information of Plaintiff and the other Class Members.

129. Each Defendant had a common law duty to prevent foreseeable harm to those who entrusted their personal, medical, and financial information to Defendants. This duty existed because Plaintiff and the other Class Members were foreseeable and probable victims of the failure of Defendants to adopt, implement, and maintain reasonable security measures so that Plaintiff's and the other Class Members' personal, medical, and financial information would not be accessible by unauthorized persons.

130. Defendants had a special relationship with the Plaintiff and the other Class Members. Plaintiff' and the other Class Members entrusted their Sensitive Information to Defendants, and each Defendant was in a position to protect this Sensitive Information from unauthorized access and activity.

131. Defendants' duties further arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the Defendants' duties.

132. As such, each Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class Members' Sensitive Information in its possession so that the Sensitive Information would not come within the possession, access, or control of unauthorized persons.

133. More specifically, Defendants' duties, included, among other things, the duty to:

A. Adopt, implement, and maintain policies, procedures, and security measures for protecting Plaintiff's and the other Class Members' Sensitive Information, including policies, procedures, and security measures;

B. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of Plaintiff's and the other Class Members' Sensitive Information with entities that failed to adopt, implement, and maintain policies, procedures, and security measures;

C. Adopt, implement, and maintain reasonable policies and procedures to ensure that Plaintiff's and the other Class Members' Sensitive Information is disclosed only with authorized persons who have adopted, implemented, and maintained policies, procedures, and security measures;

D. Properly train its employees to protect documents containing Plaintiff's and the other Class Members' Sensitive Information; and

E. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly repel breaches to the security of its systems.

134. Defendants each breached the foregoing duties and failed to exercise reasonable care in the ways described above in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and the other Class Members' Sensitive Information in its possession, custody, and care. Defendant's failure to take reasonable steps to protect the Sensitive Information of Plaintiff and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiff's and the other Class Members' Sensitive Information. This ease of access allowed thieves to steal the Sensitive Information of Plaintiff and the other Class Members, which could lead to dissemination in black markets.

135. As a direct proximate result of Defendant's conduct, Plaintiff and the other Class Members have suffered theft of their Sensitive Information. Defendant allowed thieves access to Class Members' Sensitive Information, thereby decreasing the security of Class Members' financial and health accounts, making Class Members' identities less secure and reliable, and subjecting Class Members to the imminent threat of identity theft. Not only will Plaintiff and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

136. As a direct and proximate result of the conduct of Defendants, Plaintiff and the other Class Members have suffered and will continue to suffer non-economic damages including, but not limited to, anxiety, emotional distress, and loss of privacy. Plaintiff and Class will sustain economic and non-economic damages into the future.

137. As a direct and proximate result of Defendant's collective negligence, Plaintiff and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, and punitive damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE *PER SE*
ALL DEFENDANTS
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

138. Plaintiff restates and realleges all proceeding factual allegations above and hereafter as if fully set forth herein.

139. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Elekta for failing to use reasonable measures to protect Sensitive Information. Various FTC publications and orders also form the basis of Defendants' duty.

140. Elekta violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive they obtained and stored and the foreseeable consequences of a data breach.

141. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

142. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

143. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

144. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
NEGLIGENT ENTRUSTMENT
DEFENDANT NMHC
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

145. Plaintiff incorporates by reference all other allegations in the complaint as if fully set forth here.

146. Defendant NMHC owed a duty to Plaintiff and the Class to adequately safeguard the Sensitive Information that it required Class Members to provide. Part and parcel with this duty was the duty to only entrust that data to third-party vendors with adequate and reasonable security measures and systems in place to prevent the unauthorized disclosure of such data.

147. NMHC breached this duty by entrusting Defendant Elekta with the Sensitive Information of its patients when, as described throughout the Complaint, it knew or should have known that Elekta's legacy software and cloud system was incompetent at preventing such unauthorized disclosure.

148. NMHC further breached this duty by entrusting Elekta with the Sensitive Information of the Class Members when it failed to require Elekta to implement a deletion policy where information that was not needed or no longer needed for patient medical care, patient billing, or health care operations related to Plaintiff or the Class.

149. As a direct and proximate result of Defendant's failure to exercise reasonable care in whom it entrusted the Class Members Sensitive Information to, the Sensitive Information of the Class Members was accessed by ill-intentioned criminals who could and will use the information to commit identity theft or financial fraud. Plaintiff and the Class face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their Sensitive Information.

150. As a direct and proximate result of NMHC conduct, Plaintiff and the other Class

Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the Breach and have lost time and/or money as a result of past and continued efforts to protect their Sensitive Information and prevent the unauthorized use of their Sensitive Information. Plaintiff and Class will sustain economic and non-economic damages into the future.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
DEFENDANT NMHC
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

151. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

152. Plaintiff and the Class Members entered into implied contracts with NMHC under which NMHC agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

153. Plaintiff and the Class were required to and delivered their Sensitive Information to NMHC as part of the process of obtaining services provided by NMHC. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

154. NMHC accepted possession of Plaintiff's and Class Members' Sensitive Information for the purpose of providing services or employment to Plaintiff and Class Members.

155. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with NMHC whereby NMHC became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

156. In delivering their Sensitive Information to NMHC and paying for healthcare services, Plaintiff and Class Members intended and understood that NMHC would adequately safeguard the data as part of that service.

157. In their written policies, NMHC expressly promised to Plaintiff and Class Members that it would only disclose protected information and other Sensitive Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

158. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

159. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII or PHI also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption from Bricker; and (6) other steps to protect against foreseeable data breaches.

160. Plaintiff and the Class Members would not have entrusted their Sensitive Information to NMHC in the absence of such an implied contract.

161. Had NMHC disclosed to Plaintiff and the Class that it would entrust such data to incompetent third-party agents that did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Sensitive Information to NMHC.

162. NMHC recognized that Plaintiff's and Class Member's personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

163. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with NMHC.

164. NMHC breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their data as described herein.

165. As a direct and proximate result of NMHC's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
DEFENDANT NMHC
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

166. Plaintiff incorporates by reference all other allegations in the complaint as if fully set forth herein.

167. Defendants failed to provide reasonable security, safeguards, and protections to the Sensitive Information of Plaintiff and Class Members, and as a result Plaintiff and the Class overpaid Defendant as part of the services they purchased.

168. NMHC failed to disclose to Plaintiff and Class Members that Elekta's data security practices, firewalls, and software and systems (which Elekta's chose to utilize) were inadequate to safeguard Plaintiff's and the Class Members' Sensitive Information against theft.

169. Under principles of equity and good conscience, NMHC should not be permitted to retain the money belonging to Plaintiff and Class Members because NMHC failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' Sensitive Information. Accordingly, Plaintiff and the other Class Members paid for services that they did not receive.

170. NMHC wrongfully accepted and retained these benefits to the detriment of Plaintiff

and Class Members.

171. NMHC enrichment at the expense of Plaintiff and Class Members is and was unjust.

172. As a result of Defendants' wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by NMHC, plus attorneys' fees, costs, and interest thereon.

SIXTH CAUSE OF ACTION
VICARIOUS LIABILITY
DEFENDANT NMHC
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

173. Plaintiff incorporates the previous paragraphs of this Complaint as if fully restated here.

174. At all relevant times, Elektra was the agent and/or independent contractor of NMHC

175. Defendant Elekta was negligent by failing to take adequate steps to protect the Sensitive Information that was provided by NMHC. Elekta's negligence, independently or in combination with NMHC's negligence, allowed the third-party criminals to access Plaintiff's and Class Members' PII and PHI.

176. As a direct and proximate result of the negligence of its agent, and/or independent contractor, NMHC is vicariously liable for the injuries and damages described above and Plaintiff and the Class are entitled to compensatory damages.

SEVENTH CAUSE OF ACTION
DECLARATORY JUDGMENT
ALL DEFENDANTS
(On Behalf of Plaintiff and the Nationwide Class or, alternatively, the Illinois Class)

177. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

178. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

179. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI, including whether Elekta is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII/PHI. Plaintiff alleges that Elekta's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and PHI will occur in the future.

180. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

A. Elekta owes a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach under the common law, and Section 5 of the FTC Act; and

B. Elekta continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

181. This Court also should issue corresponding prospective injunctive relief requiring Elekta to employ adequate security protocols consistent with law and industry standards to protect consumers' PII and PHI.

182. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable

injury, and lack an adequate legal remedy, in the event of another data breach at Elekta. The risk of another such breach is real, immediate, and substantial. If another breach at Elekta occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

183. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Elekta if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Elekta of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Elekta has a pre-existing legal obligation to employ such measures.

184. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Elekta, thus eliminating the additional injuries that would result to Plaintiff and consumers whose PII and PHI would be further compromised.

EIGHTH CAUSE OF ACTION
VIOLATION OF ILLINOIS GENETIC INFORMATION PRIVACY ACT ("GIPA")
(410 ILCS 513)
DEFENDANT ELEKTA
(On Behalf of Plaintiff and the Illinois Class)

185. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

186. Genetic testing and genetic information is confidential and privileged and may only be released to the individual tested and to persons specifically authorized by that individual in writing.

187. Genetic information can be valuable to the individual and to criminal markets and

includes the following:

A. Individuals genetic tests related to an analysis of human DNA, RNA, chromosomes, proteins, or metabolites;

B. The genetic tests of family members of the individual;

C. The manifestation of a disease or disorder in family members;

D. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, the individual or any family member or such individual. [46]

188. Genetic services means: (1) a genetic test; (2) genetic counseling (including obtaining, interpreting, or assessing genetic information); or genetic education. [47]

189. Genetic testing means an analysis of human DNA, RNA, chromosomes, proteins or metabolites, if the analyses detects genotypes, mutations, or chromosomal changes. [48] This includes tests that would be administered for BRCA1, BRCA2, colorectal genetic variant and other genetic tests provided to cancer patients.

190. Plaintiff and Class Members allowed for genetic information derived from genetic testing to be acquired by and stored at NMMC with the expectation that the genetic test results and genetic information would not be disclosed without consent.

191. Upon information and belief, such genetic information was contained within cloud system that were hosted by Elektra and subject to the Data Breach at issue.

192. Elekta violated this act by negligently and recklessly disclosing the genetic information to criminal third parties as described herein by releasing, transferring, providing

[46] 45 CFR 160.103
[47] *Id.*
[48] *Id.*

access to, divulging through its affirmative negligent actions and omissions Plaintiffs and Class Members Genetic Information to criminal third parties outside the entity.

193. As a direct and proximate result of the unauthorized disclosure of Plaintiff and Class Members genetic information, Plaintiff and the Class have suffered actual damages as described herein and liquidated damages under 410 ILCS 513.40.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as a representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Statutory damages under 410 ILCS 513.40

g. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

h. Awarding pre- and post-judgment interest on any amounts awarded: and

Awarding such other and further relief as may be just and proper

DEMAND FOR JURY TRIAL

Plaintiff individually and on behalf of all others similarly situated, hereby demands a trial by jury on all claims so triable.

Respectfully submitted,

/s/ Joseph M. Lyon
Joseph Lyon (OH-0076050)
THE LYON FIRM, LLC
2754 Erie Ave
Cincinnati, Ohio 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com

/s/ Daniel Zemans
Daniel Zemans (ARDC 6284309)
Law Offices of Daniel Zemans, LLC
2023 W. Berteau Avenue
Chicago, IL 60618
Phone: (773) 706-7767
dzemans@zemans-law.com

Counsel for Plaintiff and the putative Class